QUERY DATA PACKET PROCESSING AND NETWORK SCANNING METHOD AND APPARATUS

ABSTRACT OF THE DISCLOSURE

A method for detecting within a networked computer a target vulnerability such as a Trojan Horse residing therein is disclosed, wherein the vulnerability is characterized by a signature response to an encrypted query. The method includes encrypting a plurality of query data packets in accordance with a plurality of encryption keys, each encrypted query data packet including a defined query field specific to the target vulnerability. The method further includes storing the plurality of encrypted query data packets in a memory. The method further includes thereafter scanning the networked computer for a target vulnerability residing within the networked computer by sending successive ones of the encrypted-and-stored query data packets to the host computer and analyzing responses thereto from the host computer with respect to the characteristic signature. Preferably, the encrypting is performed for substantially all of the encryption keys within a defined key space. The memory may be non-volatile memory such as a disk drive or a volatile memory such as random-access memory (RAM) or a memory configured as a cache.